



## COUNTY OF LOS ANGELES

### CHIEF INFORMATION OFFICE


500 West Temple Street  
493 Kenneth Hahn Hall of Administration  
Los Angeles, CA 90012

JON W. FULLINWIDER  
CHIEF INFORMATION OFFICER

Telephone: (213) 974-2008  
Facsimile: (213) 633-4733

October 22, 2004

To: Supervisor Don Knabe, Chairman  
Supervisor Gloria Molina, Chair Pro Tem  
Supervisor Yvonne Brathwaite Burke  
Supervisor Zev Yaroslavsky  
Supervisor Michael D. Antonovich

From: Jon W. Fullinwider   
Chief Information Officer

Subject: **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT  
(HIPAA) INFORMATION SECURITY ASSESSMENT - INFORMATION  
TECHNOLOGY SUPPORT SERVICES MASTER AGREEMENT WORK  
ORDER**

This is to notify you of my intent to request the Internal Services Department (ISD) to execute a Work Order for an amount not to exceed \$800,000, under the Information Technology Support Services Master Agreement (ITSSMA). This Work Order is requesting a HIPAA Information Security Risk Analysis be conducted to identify potential risks of unauthorized exposure of Health Insurance Portability and Accountability Act (HIPAA) data that is in electronic form.

In accordance with ITSSMA Guidelines, prior Board notice is required for projects that will exceed \$300,000. This request is to obtain independent and technically skilled information security and audit personnel with HIPAA expertise to perform a security assessment and risk analysis for the covered entities.

### BACKGROUND

The planned risk analysis is required to comply with the HIPAA Security Rules as published in the Federal Register and requiring compliance by April 20, 2005. This legislation affects four (4) County departments [Health Services, Mental Health, Probation (limited to the Dorothy Kirby Center), and the Sheriff (limited to the Pharmaceuticals)] that your Board designated as covered entities under this legislation.

The project supported by this ITSSMA contract is critical to identifying compliance with the HIPAA Security Rules Standard that includes three critical safeguard components: administrative, technical, and physical. The County's Chief Information Security Officer (CISO) will provide contractor direction and project oversight, while coordinating with Project Managers that have been assigned by each affected department. The contracted team will be tasked to perform a security assessment and risk analysis to determine deficiencies that are specific to each "covered entity".

## **SCOPE OF WORK**

In order to ensure compliance with the HIPAA Security Rules, the selected contractor will perform activities to determine areas requiring security improvements to comply with HIPAA requirements. The engagement will include interviews of departments' key personnel, processing of information technology tools and techniques, conducting audits of certain processes, and review of policies, standards and procedures. The assessment results will be disseminated to the CISO and appropriate County department management for planned remediation, which includes development and implementation of policies, procedures, or processes.

The selected contractor will use their technical information security and audit experience, as well as their HIPAA knowledge to perform a security assessment and risk analysis for the aforementioned departments. The contractor will determine gaps and risks associated with the HIPAA Security Rules and evaluate them based on the specific department environment to provide recommended corrective actions. The contractor will provide various reports that include a gap and vulnerability analysis that correlates a risk level for the existing technology, process, or procedures.

## **JUSTIFICATION**

The covered entity departments participating in this Work Order do not have sufficient personnel to perform the tasks required without the assistance of a contractor's team. In addition, County personnel are not available to provide essential functions with the required expertise, experience, and knowledge associated with HIPAA Rules. Consequently, we are seeking use of ITSSMA to supplement the existing I/T staff. The vendors available under ITSSMA have extensive knowledge and expertise with information security and HIPAA, which are knowledge and skills required to successfully complete this Work Order.

The services proposed under this ITSSMA Work Order are essential to providing the "covered entities" the contract services required to determine and measure compliance with the HIPAA Security Rules.

The completion of a information security risk assessment is a requirement under the provisions of the HIPAA Security Rules. The size of the County's "covered entities" requires the use of consultants to complete the task prior to the April 20, 2005 compliance deadline.

## **FISCAL IMPACT**

The HIPAA Rules have civil and criminal penalties if an organization does not demonstrate due diligence in achieving and maintaining compliance. Organizations that do not comply with the HIPAA Security Rules requirements are subject to a number of penalties. The civil penalties are \$100 per violation, up to \$25,000 per year for each requirement violated. Criminal penalties range from \$50,000 in fines and one year in prison up to \$250,000 in fines and 10 years in jail.

The cost of the proposed Work Order will be prorated between the four (4) affected departments [Department of Health Services, Department of Mental Health, Probation (The Dorothy Kirby Center) and the Sheriff (Pharmaceuticals)]. These departments will fund the consulting engagement from their Fiscal Year 2004-05 Budgets. Subsequently, each department will have to fund correction of identified deficiencies documented in the risk assessment.

## **NOTIFICATION TIMELINE**

In accordance with the ITSSMA policies and procedures, I will delay my request for the Internal Services Department to execute this work order, for two weeks pending any questions or direction to the contrary by your Board.

If you have questions or require additional information, please feel free to contact me at (213) 974-2008 or, in my absence, you may contact Mr. Al Brusewitz, Chief Information Security Officer at (562) 940-3873.

JWF:RP:ygd

c:     Executive Officer, Board of Supervisors  
        Chief Administrative Officer  
        County Counsel  
        Interim Director, Internal Services Department  
        Chair, ISC